State of Maine
Department of Administrative & Financial Services
Office of Information Technology (OIT)

Vulnerability Scanning Procedure (RA-5)

Table of Contents

1.0. Purpose

1.1. The purpose of this document is to define OIT's procedures for assessing Cybersecurity vulnerabilities through proactive scanning of Information Assets and addressing any discovered vulnerabilities in a timely fashion. It falls under the umbrella Risk Assessment Policy. More specifically, this document corresponds to the Control RA-5[1], including Control Enhancement (CE) numbers 1 through 3, and 5, of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).

2.0. Scope

2.1. This document applies to:

2.1.1. All State of Maine personnel, both employees and contractors;

2.1.2. Executive Branch Agency information assets, irrespective of location; and

2.1.2. Information assets from other State government branches that use the State network.

3.0. Conflict

3.1. If this document conflicts with any law or union contract in effect, the terms of the existing law or contract prevail.

4.0. Procedures

4.1. For OIT-hosted Information Assets, OIT Information Security executes the vulnerability scans.

4.2. For Externally-hosted Information Assets, OIT Information Security either executes the vulnerability scans, or collects vulnerability scans from vendors, or other third-party auditors.

4.3. OIT Information Security distributes the scan results, on a need-to-know basis, to the downstream partners, and works with them to filter out the false-positives and false-negatives, thereby identifying all legitimate vulnerabilities. The downstream partners and/or Information Asset owners include:

4.3.1. OIT Client Technologies;

4.3.2. OIT Network Services;

4.3.3. OIT Computing Infrastructure and Services;

4.3.4. OIT Data Services; and

4.3.5. OIT Application Divisions.

4.4. The downstream partners listed above remediate all legitimate vulnerabilities within their span-of-control, within the prescribed remediation schedule. They also collaborate with OIT Information Security in exploring Compensating Controls should outright remediation turn out to be elusive.

[1] https://nvd.nist.gov/800-53/Rev4/control/RA-5

4.5. OIT Information Security also liaises with horizontal Industry Partners on a need-to-know basis to help contain similar vulnerabilities in the wild. This includes MS-ISAC[2], the Maine Information and Analysis Center[3] (which then interfaces with state, local, and federal law-enforcement partners).

4.6. OIT Vendor Management holds all vendors/partners for Externally-hosted Information Assets accountable to this Procedure, within the vendor/partner's span-of-control.

4.7. OIT Account Management owns the Agency Business Customer interface related to this Procedure.

4.8. By default, Vulnerability Scanners classify vulnerabilities into three risk tiers: Low, Medium, and High. Even if a Vulnerability Scanner uses a different taxonomy in its output, OIT Information Security will translate that output into the standard Low-Medium-High tier structure, according to the following meanings:
4.8.1. Low: No direct compromise of Cybersecurity.
4.8.2. Medium: Measurable, but limited, compromise of Cybersecurity.
4.8.3. High: Severe compromise of Cybersecurity.

4.9. The default OIT vulnerability remediation schedule is as follows:
4.9.1. For *new* Information Assets:
4.9.1.1. High-Risk vulnerabilities must be remediated *prior to production deployment.*
4.9.1.2. Medium-Risk vulnerabilities must be remediated *prior to production deployment.*
4.9.1.3. Low-Risk vulnerabilities must be remediated in alignment with the natural product lifecycle (version & release upgrades, patch lifecycle, etc.).
4.9.2. For *established* Information Assets:
4.9.2.1. High-Risk vulnerabilities must be remediated within 30 calendar days of identification of the vulnerabilities*.*
4.9.2.2. Medium-Risk vulnerabilities must be remediated within 90 calendar days of identification of the vulnerabilities*.*
4.9.2.3. Low-Risk vulnerabilities must be remediated in alignment with the natural product lifecycle (version & release upgrades, patch lifecycle, etc.).

4.10. Irrespective of the default Risk Classification, and the default remediation schedule, specified above, for any specific vulnerability, the CISO may impose a different classification, and/or different a remediation schedule.

[2] https://www.cisecurity.org/ms-isac/

[3] https://memiac.org/

4.11. Typically, vulnerabilities are remediated by applying vendor-supplied patches, or updating custom code. However, under certain circumstances, Compensating Controls may be used as an alternative until the next maintenance/patching schedule. The CISO remains the final arbiter re: whether a Compensating Control does quality as remediation, and the timeframe thereof.

4.12. The Vulnerability Scanners must be upgraded no less frequently than once per calendar week, *and* when new vulnerabilities are flagged by industry partners. **(RA-5(1), RA-5(2))**

4.13. The Vulnerability Scanners utilized by OIT are industry-leading products, and, at a minimum, they are configured for **(RA-5(3), RA-5(4))**:

4.13.1. the CIS (Center for Internet Security) Benchmarks for Configurations[4];
4.13.2. Missing Original Vendor patches;
4.13.3. Missing third-party, commodity application (such as from Adobe, Oracle-Java, and others) patches;
4.13.4. Misconfigurations in third-party, commodity applications (such as from Adobe, Oracle-Java, and others), as recommended by the product vendors, and/or Industry Partners;
4.13.5. Functions, Services, Ports, and Protocols that should be disabled, or restricted, as recommended by the product vendors, and/or Industry Partners;
4.13.6. Higher sensitivity toward Information Assets that are discoverable from the Internet;
4.13.7. Higher sensitivity toward the potential for Privilege Escalation;
4.13.8. Higher sensitivity toward the potential for Information Leakage;
4.13.9. Industry-standard output, in terms of the Common Vulnerabilities and Exposures (CVE)[5], the Open Vulnerability and Assessment Language (OVAL)[6], the Common Weakness Enumeration (CWE)[7], the National Vulnerability Database (NVD)[8], the Common Vulnerability Scoring System (CVSS)[9], etc.;
4.13.10. For web-based applications, vulnerability standards include OWASP[10], SAFECode[11], BSIMM[12], the Cloud Security Alliance[13], etc.

[4] https://www.cisecurity.org/cis-benchmarks/
[5] https://cve.mitre.org/
[6] https://oval.mitre.org/
[7] https://cwe.mitre.org/
[8] https://nvd.nist.gov/
[9] https://www.first.org/cvss/
[10] https://www.owasp.org/
[11] https://safecode.org/
[12] https://www.bsimm.com/
[13] https://cloudsecurityalliance.org/

4.14. At a minimum, the Vulnerability Scans use both Unauthenticated (black-box) and Authenticated (white-box) scans. Depending on the criticality of the target system, the Authenticated scans may be further broken down into two: Regular User Access, and Administrative/Privileged Access. If an Information Asset allows Role-Based Access Control, then all major roles must be exercised in the Authenticated testing as well. **(RA-5(5))**

4.15. Scanning Frequency:

4.15.1. OIT-hosted Infrastructure is scanned at Infrastructure Deployment Certification[14], when new vulnerabilities potentially affecting such Information Assets are reported by Industry Partners, and whenever a major upgrade to such an Information Asset is performed. Additionally:

4.15.1.1. Servers (including server-based backup components), appliances, and networking gear are scanned at least once per month.

4.15.1.2. Databases are scanned at least once per quarter.

4.15.1.3. Perimeter firewalls are scanned routinely by the Federal Department of Homeland Security, which also provides weekly reports.

4.15.1.4. Endpoint workstations undergo local vulnerability scans once every six (6) hours.

4.15.1.5. Endpoint mobile devices are managed via a mobile endpoint security application.

4.15.2. OIT-hosted Applications are scanned at Application Deployment Certification[15], and, at least, once every calendar year subsequently. They are also scanned at every major upgrade, and when new vulnerabilities potentially affecting such Applications are reported by Industry Partners.

4.15.3. Externally-hosted Information Assets are scanned at the relevant Deployment Certification (Infrastructure or Application), and once every calendar year subsequently. They are also scanned at every major upgrade, and when new vulnerabilities potentially affecting such Information Assets are reported by Industry Partners. Depending upon the specific contractual terms, either OIT Information Security does the scanning, is provided a scan by the vendor, or a third-party auditor provides the scan.

4.16. Any vulnerability remediation (including instituting Compensating Controls) on any Information Asset involves testing, and it potentially impacts Agency Business partners. OIT must coordinate all Agency Business partners liaison through the Account Mangers. Agencies cooperate with OIT on User Acceptance Testing for the remediation of legitimate vulnerabilities.

[14] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/infrastructure-deployment-certification.pdf

[15] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification_0.pdf

4.17. Any necessary configuration change must be managed as outlined in Change Management Policy[16].

4.18. OIT employs an industry-leading Security Information & Event Management (SIEM) system, in order to: **(RA-5(6), RA-5(8), RA-5(10))**

4.18.1. Compare the results of vulnerability scans over time to determine trends in information system vulnerabilities;

4.18.2. Review historic audit logs to determine if a vulnerability identified in the information system has been previously exploited; and

4.18.3. Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.

4.19. Should there occur a High-Risk legitimate vulnerability in an Information Asset that is not amenable to timely remediation or a compensating control, the CISO may instruct the cessation-of-operation of the said Information Asset, until the risk is mitigated to the satisfaction of the CISO.

5.0. Records Management

5.1. Office of Information Technology security policies, plans, and procedures fall under the *Routine Administrative Policies and Procedures and Internal Control Policies and Directives* records management categories. They will be retained for three (3) years, and then destroyed in accordance with guidance provided by Maine State Archives. Retention of these documents will be subject to any future State Archives General Schedule revisions that cover these categories.

6.0. Public Records Exceptions

6.1. Under the Maine Freedom of Access Act, certain public records exceptions may limit disclosure of agency records related to information technology infrastructure and systems, as well as security plans, procedures or risk assessments. Information contained in these records may be disclosed to the Legislature, or, in the case of a political or administrative subdivision, to municipal officials or board members under conditions that protect the information from further disclosure. Any aggrieved person seeking relief for an alleged violation of the FOAA may bring suit in any Superior Court in the state.

7.0. Document Details

7.1. Initial Issue Date: 6 March 2020

7.2. Latest Revision Date: 6 March 2020

7.3. Point of Contact: Enterprise.Architect@Maine.Gov

7.4. Approved By: Chief Information Officer, OIT

7.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[17]

[16] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/change-management-policy.pdf

[17] https://legislature.maine.gov/statutes/5/title5ch163sec0.html

7.6. Waiver Process: Waiver Policy[18]

8.0. Definitions

8.1. *Compensating Control:* An alternative mechanism instituted to mitigate a legitimate vulnerability when the actual mechanism to properly remediate the vulnerability is deemed impractical in the present time. If utilized, Compensating Controls must provide the same, or greater level, of defense as would be attained through the proper remediation. Compensating Controls may be used as an interim solution, until the full remediation can be undertaken.

8.2. *Externally-hosted Information Assets:* Generic term for any I.T. product consumed from the Public Cloud. Includes the full spectrum of Software as a Service, Platform as a Service, and Infrastructure as a Service.

8.3. *Industry Partner:* Generic term for *all* external parties that apprise the Information Security Division of the Cybersecurity vulnerability landscape. Could be open-channel partners, such as product vendors, trade magazines, security research organizations, etc. Could be closed-channel partners, such as MS-ISAC, the Maine Information and Analysis Center, et al.

8.4. *Information Assets:* The full spectrum of all I.T. products, including business applications, system software, development tools, utilities, appliances, etc.

8.5. *Legitimate Vulnerability*: Neither a false positive, nor a false negative. An actual weakness, not only flagged by an automated scan, but verified by a human analyst.

8.6. *Vulnerability:* Weakness in an Information Asset that could be exploited by a threat source.

8.7. *Vulnerability Scanner:* A specialized application custom-built to detect, and report out, vulnerabilities. Examples include Tenable Nessus, HCL/IBM AppScan, etc.

[18] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf